REMARKS

Status of the Claims

In the Office Action, claims 1-22 are noted as pending in the application. All claims stand rejected.

A. Summary of Cited References

Before addressing the Examiner's rejections, a brief summary of the cited references is provided.

Heer - U.S. Patent Number 6,028,933

Heer relates to encryption of signals from and to multiple units over a broadband network. Title. The invention discussed in Heer uses a virtual random number generator at a cable modem to reduce cable modem hardware. An authentication and key generation process between the head end and cable modem produces a mutually authentication and mutually generated permanent key. Abstract. In reference to FIG. 29, a connection key (CCK) is generated from a mutually authenticated [by cable modem and head end] permanent key. Col. 34, lines 12-14. A secret key is negotiated between and shared by a cable modem and head end equipment. Col. 34, lines 15-20. The CCK is also a secret key, but is replaced each time a new connection is established between the cable modem and the head end, or if a current CCK is a week old. Col. 34, lines 21-23.

B. Examiner's Response to Arguments

Examiner has maintained the rejection made in the previous office action. Since the rejection appears to be verbatim the same as previously made, Applicant provides a verbatim response as provided in the previous Amendment. In addition to the reproduced remarks made in response to the previous office action, applicant herein responds to Examiner's Response to Arguments made in the current office action.

Examiner states that he disagrees with Applicant's argument that Heer does not teach a new key is generated and transmitted with each communication between a cable modem and a head end device. Only for the purpose of discussing and replying to Examiner's arguments, Applicant accepts Examiner's statement that Heer teaches that a new session key is generated and used upon each new connection being established between a cable modem and the head end. Also for purposes of discussion, Applicant accepts that Heer teaches that one session may comprise one or more data exchanges. Indeed, many exchanges of data elements occur during the course of one session. Likewise, Applicant accepts for the purposes of discussion that a communication may comprise only one data exchange. Also, Applicant accepts for the purpose of discussion that when a session ends, the session key for the just-ended session is destroyed. Thus, Applicant accepts, for the purposes of discussion, that all of these statements made by Examiner are correct.

However, Examiner has not advanced a logical argument how these statements show that Heer anticipates claim 1. None of these statements show that a new key is generated for each communication. Coupling these statements with Examiner's statement that the claims do not recite that packets and frames are basic data elements of communications, Examiner seems to be asserting that a session is the same as a communication is the same as a data exchange. For example, the server generates a new

seed at step E in claim 1 based on the new key received from first client modem at the server in step B. In this sequence recited in claim 1 it is clear that a new seed, which will be used to generate another new key at the client cable modem, is generated based on a new key in a scrambled packet received at the server at step B. In short, each upstream packet and downstream subpacket transmitted during a session contains a new key that is encrypted by the sending device using a seed already known to both the sending and receiving deivces. These features are expressly recited in claim 1, and the other independent claims.

To help clear up any confusion regarding what a communication is, Applicant has amended the claims so that, with the exception of claim 19, the independent claims recite that a downstream communication is a subpacket and an upstream communication is a packet. In claim 19, a communications in either upstream or downstream direction is recited as a packet.

Based on the concept recited in claim 1 that a new key associated with a particular client modem with which the server is communicating is embedded into each packet sent from the client modem to the server, or in each subpacket sent from the server to the client modem, claim 1 distinguishes over the Heer reference. As Examiner stated, and Applicant has acknowledged, Heer teaches that a new key is generated for each new session or after a week if a session has not been terminated one week after it began. This key is referred to as a CCK, and is generated based on another key, PKM, which is shared between the CM and the head end and should remain secret for the practical lifetime of the cable modem, typically twenty years. Col. 34, lines17-23. Therefore, Heer does not teach that a new key is generated for each packet, or subpacket, that is communicated between a client modem and a server. Withdrawal of the rejection is respectfully requested. In addition, since the other independent claims include similar limitations of claim 1, similar analysis as given above with respect to claim 1 applies to them. Withdrawal of the rejection is respectfully requested. Furthermore, the dependent claims include all of the limitations of the independent claims from which they depend. Therefore, since the independent claims patentably distinguish over the reference, they too distinguish over the reference. Withdrawal of the rejection is respectfully requested.

Applicant made the following remarks in the previous Amendment and are provided below for Examiner's convenience.

C. Rejection of Claims under 35 U.S.C. § 102(e).

Regarding the rejection of independent claims 1 and 14, which share some scope and subject matter, claim 1 recites in element B unscrambling an upstream communication containing a new key using a "previous seed for [a] modem based on a previous key for the [] modem [that was] received in a previous [] communication from the [] modem." A new seed corresponding to the new key is used, as recited in element E, to scramble a next downstream communication to the modem. When the modem sends a next upstream communication, yet another key, referred to as a next key, is included therein as recited in element H. The next communication is scrambled using the new seed before being transmitted upstream, as recited in element J.

Heer does not recite these limitations. As discussed above, Heer relates to using a permanent private key to encrypt packets within a session. Moreover, Heer discloses that

a new session key is created at the beginning of a new session, or if the current session key is more than a week old. One skilled in the art will appreciate that a session begins upon registration of the cable modem with the head end. The session typically ends when the user logs off, power is lost at either the cable modem or head end equipment, or a physical break in a network link occurs.

In contrast, according to claim 1, upon each communication between the cable modem and head end, a new key is generated and transmitted with the payload of the communication. As defined in the specification, a communication includes a CRC value for providing a transmission check word. Page 12, lines 15-23. As described in this passage, the CRC value is placed in a sub-packet, which is part of a frame. One skilled in the art will appreciate that the terms packet and frame describe portions of basic data elements of digital communication. Thus, the term 'communication' in the present application refers to a data element, of which many are transmitted in a second and clearly more than once per session. Therefore, claim 1 recites forming a unique (inasmuch as a pseudo random generator always generates random values) key and corresponding seed for every basic data element that is transmitted between a cable modem and head end equipment. This is supported in the specification at page 16, lines 19-27 for a communication in the downstream direction. As discussed above, Heer clearly teaches away from this because a new key is only generated at the start of a new session or once per week. Since all of the elements claimed in the claim are not found in the reference, withdrawal of the rejection of claims 1 and 14 is respectfully requested.

With respect to claim 15 and 19, similar analysis as to claims 1 and 14 applies inasmuch as when one device sends a communication to the other, the communication is encrypted based on a key received in the previous communication from the other device. As discussed above, this distinguishing feature is not found in Heer, because Heer teaches using a permanent key that is used for many communications, for up to one week, whereas in claims 15 and 19, each communication, or packet frame, includes a new key in reference to the previous communication. Thus, the claims patentable distinguish over the reference. Withdrawal of the rejection is respectfully requested. In addition, each dependent claim contains all of the limitation of the base claim from which it depends. Therefore, the dependent claims rejected as being anticipated patentably distinguish over the reference because the base claims from which they depend patentably distinguish over the reference. Withdrawal of the rejection is respectfully requested.

Regarding the argument advanced in the previous Amendment that Heer does not disclose that a communication is encrypted based on a key received in a previous communication from another device when one device sends a communication to the other, Examiner disagrees. Examiner states that Heer discloses a key exchange between the cable modem and the head end "prior" to a flow of information. "[E]xaminer interprets the key exchange method of Heer as a key is exchanged between the cable modem and the head end prior to any transmission of data." (Emphasis added). "Once the cable modem or the head end receives the key, the cable modem/head end uses the key to encrypt the communication among them." Current office action page 3.

Thus, rather than proving Applicant's reasoning as faulty, Examiner has provided support for Applicant's position.

D. Rejection of Claims under 35 U.S.C. § 103(a).

Applicant respectfully submits that the subject matter of the claims patentably distinguish over the cited references. Under MPEP § 2142, for an examiner to establish a *prima facie* case of obviousness, "three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Applicant's disclosure." If any of these three criteria are not met, the Examiner has not met the burden of establishing a *prima facie* case of obviousness, and the rejection should be withdrawn.

Furthermore, each dependent claim includes all of the limitations of the independent claim from which it depends. If an independent claim is non-obvious under 35 U.S.C. § 103, then any claim depending therefrom is non-obvious. MPEP §2143.03, citing In re Fine, 837 F.2d 1071 (Fed. Cir. 1988). Applicant respectfully submits that the burden of establishing a *prima facie* case of obviousness has not been met.

E. The Claims are not Obvious over the Cited References

Starting on page 5 of the Office Action, claims 3, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16-18, 19-22 are rejected under 35 U.S.C. § 103 as being obvious over Heer, U.S. Patent Numbers 5,432,850 to Rothenberg, ("Rothenberg"), and 5,787,483 to Jam, et. al. ("Jam") in various combinations. The reasons that the claims patentably distinguish over the reference are addressed below.

As discussed above with respect to the rejection under 35 U.S.C. § 102, Heer does not disclose that a communication is encrypted based on a key received in a previous communication from another device when one device sends a communication to the other. The passages cited by Examiner in Jam discuss DES key exchange, which uses the Diffie-Hellman key exchange algorithm. As known in the art, Diffie-Hillman is used to compute a shared secret key for use between devices for a given session. Col. 13, lines 51-57; col. 14, lines 58-67 and col. 26, lines 17-21. Furthermore, as known in the art, the DES scheme typically uses the same secret key for more than one communication, or packet frame.

As claimed in step/element L of claim 15, the server receives an upstream communication and unscrambles it based on a previously stored key created by the modem and a previously created and stored key created by the server. In Jam (as well as Heer) different seeds and keys are not generated/stored/used at each transmission of a communication. This process, which is repeated in the other direction (from server to modem) in step/element P, continues with each communication sent between the devices, until a break in the communication is sensed, as claimed in the portion of claim 15, as amended, that recites "REPEAT steps K through Q UNTIL detecting a break in the communications between the first client modem and the server; THEN GOTO Step B." As discussed above, the encryption discussed in the cited references uses keys at least for the duration of a session, unless the session lasts longer than a week, as discussed in

Heer.

With respect to Rothenberg ("Roth"), Roth discusses encrypting messages using the destination and/or source addresses of the communicating devices over an Ethernet connection. Col. 3, lines 47-62. Thus, the value(s) is/are used to encrypt/decrypt messages do not vary per transmission.

Based on the above discussion of the cited references generally, all of the limitations of independent claims 14, 15 and 19 are not found in the references because the references all discuss a permanent, or semi permanent key for encrypting, but do not teach the creating and using of new unique keys for each data frame transmission/reception for encrypting/decrypting.

Furthermore, a motivation to combine the references is not found in the references. Lastly, combination of the cited references cannot result in a likelihood of success in achieving the claimed subject matter because, generally, the independent claims claim using seeds to encrypt/decrypt every frame, where each seed is based off of a key that is generated for a previous transmission based on a random number generator, or a pseudo-random number generator.

All of the cited references teach encrypting data either based on a key, or keys, that remain the same throughout a given session, or based on the addresses of the communicating devices, addresses of which do not change from frame transmission to frame transmission. Thus, the independent claims patentably distinguish over the reference. Withdrawal of the rejection of the independent claims is respectfully requested.

Furthermore, since every dependent claim contains all of the limitations of the base independent claim from which it depends, all of the dependent claims also patentably distinguish over the cited references. Withdrawal of the rejection is respectfully requested.

SUMMARY

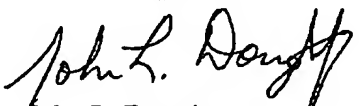
For all the reasons advanced above, Applicant respectfully submits that the application is in condition for allowance and that action is earnestly solicited.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any informalities that can be corrected by an Examiner's amendment please contact the undersigned at the mailing address, telephone, facsimile number, or e-mail address indicated below.

Arris Group, Inc.
3871 Lakefield Drive
Suwanee, Georgia 30024
(678) 473-8697
(678) 473-8095 - fax
john.doughty@arrisi.com

Respectfully submitted,

Arris Group, Inc.



John L. Doughty
Reg. No. 47,533